THREATS TO OFFSHORE ENERGY SYSTEMS

CRAIG CONKLIN, ASSOCIATE DIRECTOR

INFRASTRUCTURE ASSESSMENTS AND ANALYSIS

Cybersecurity and Infrastructure Security Agency (CISA)

VISION

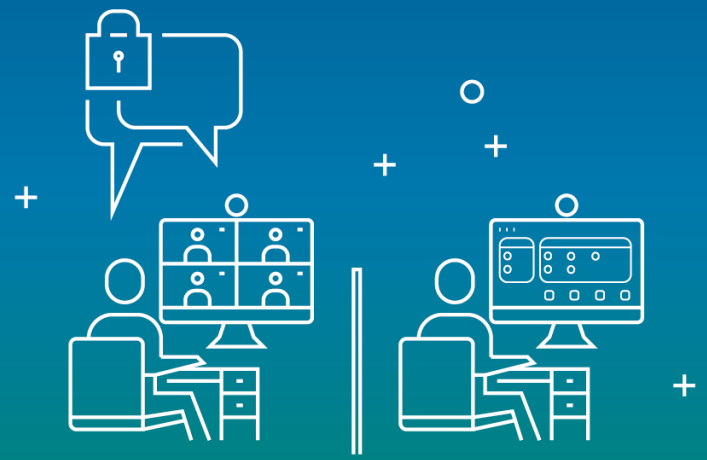
Secure and resilient infrastructure for the American people.

MISSION

Lead the national effort to understand, manage, and reduce risk to the nation's cyber and physical infrastructure.

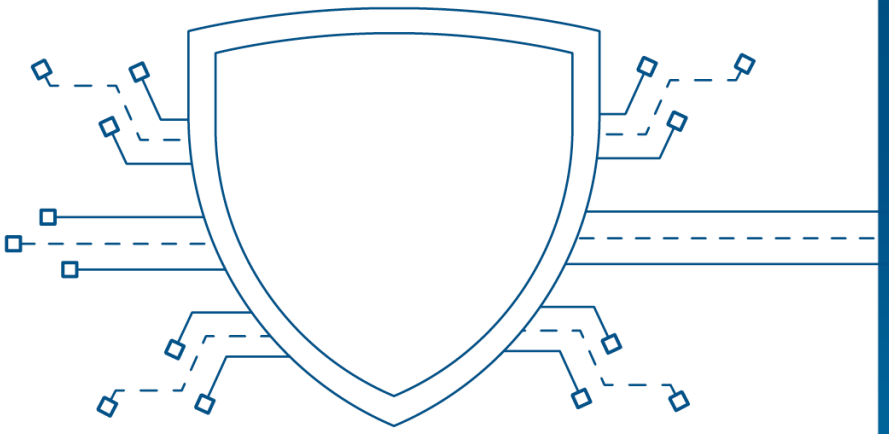
CISA's Core Capabilities

AT A GLANCE



- PARTNERSHIP DEVELOPMENT
- INFORMATION AND DATA SHARING
- CAPACITY BUILDING
- INCIDENT MANAGEMENT & RESPONSE
- RISK ASSESSMENT AND ANALYSIS
- NETWORK DEFENSE
- EMERGENCY COMMUNICATIONS

CISA's Cybersecurity Mission



CYBERSECURITY MISSION

CISA drives and enables effective national cyber defense, resilience of national critical functions, and a robust supporting ecosystem.

HOW CISA IS CARRYING OUT ITS CYBERSECURITY MISSION:

- Mature Operational Collaboration
- Expand Operational Visibility
- Drive Progress to Secure Federal Civilian Networks
- Pursue Stronger Security at Scale
- Expand Access to CISA Capabilities

CISA's Infrastructure Security Mission

INFRASTRUCTURE SECURITY MISSION

CISA leads the coordinated effort to reduce risks posed to our critical infrastructure, whether from man-made or natural causes.

HOW CISA IS CARRYING OUT ITS INFRASTRUCTURE SECURITY MISSION:

- Combat Domestic Violent Extremism
- Refreshing the National Infrastructure Protection Plan (The National Plan) and Implementing the 2021 National Defense Authorization Act (NDAA) Section 9002
- Chemical Security

CISA's Emergency Communications Mission

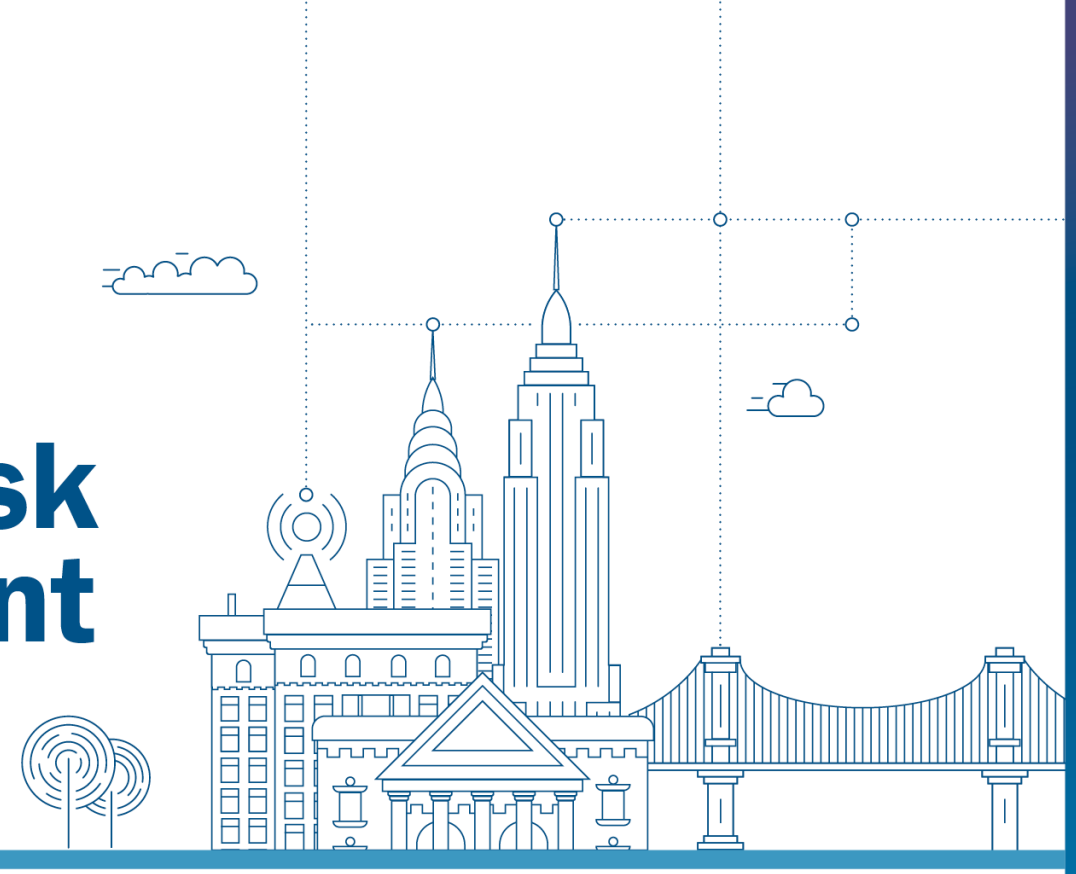
EMERGENCY COMMUNICATIONS MISSION

CISA supports and promotes communications used by emergency responders and government officials to keep America safe, secure, and resilient.

HOW CISA IS CARRYING OUT ITS EMERGENCY COMMUNICATIONS MISSION:

- Nationwide Interoperability
- Effective Communications Planning
- Moving Information with Interoperable Priority

National Risk Management Center



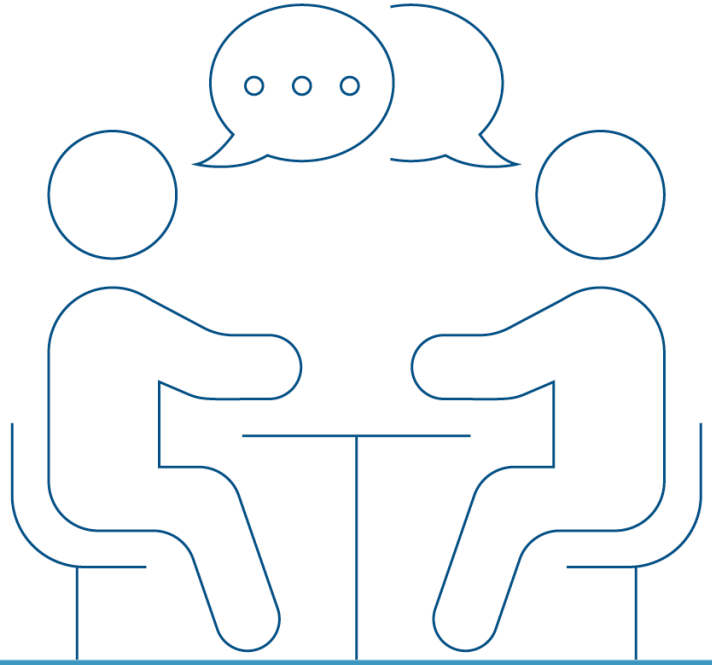
NATIONAL RISK MANAGEMENT CENTER

CISA provides provides planning, analysis, and collaboration to lead strategic risk reduction efforts for the nation.

HOW CISA IS CARRYING OUT ITS RISK MANAGEMENT MISSION:

- Collaboration
- Interconnectedness
- Focus on a Core Set of Strategic Risks

Stakeholder Engagement Mission



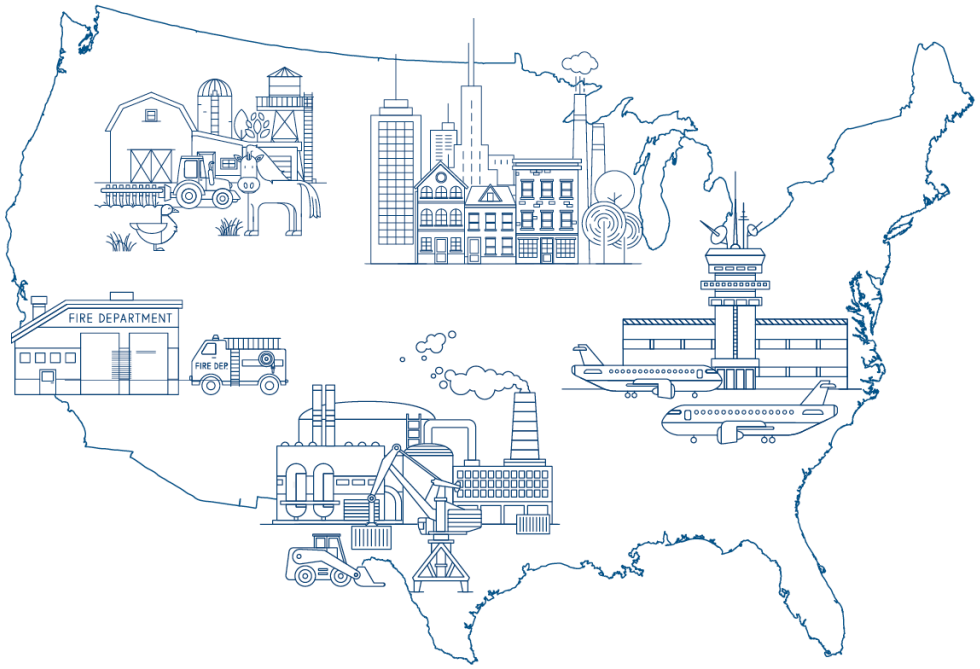
HOW CISA IS CARRYING OUT ITS STAKEHOLDER ENGAGEMENT MISSION:

- Global Outreach
- Information Sharing and Unified Engagement

STAKEHOLDER ENGAGEMENT MISSION

CISA builds and maintains national and international partnerships and engagements while serving as the hub for the shared stakeholder information that advances unified risk reduction efforts.

Integrated Operations Mission



INTEGRATED OPERATIONS MISSION

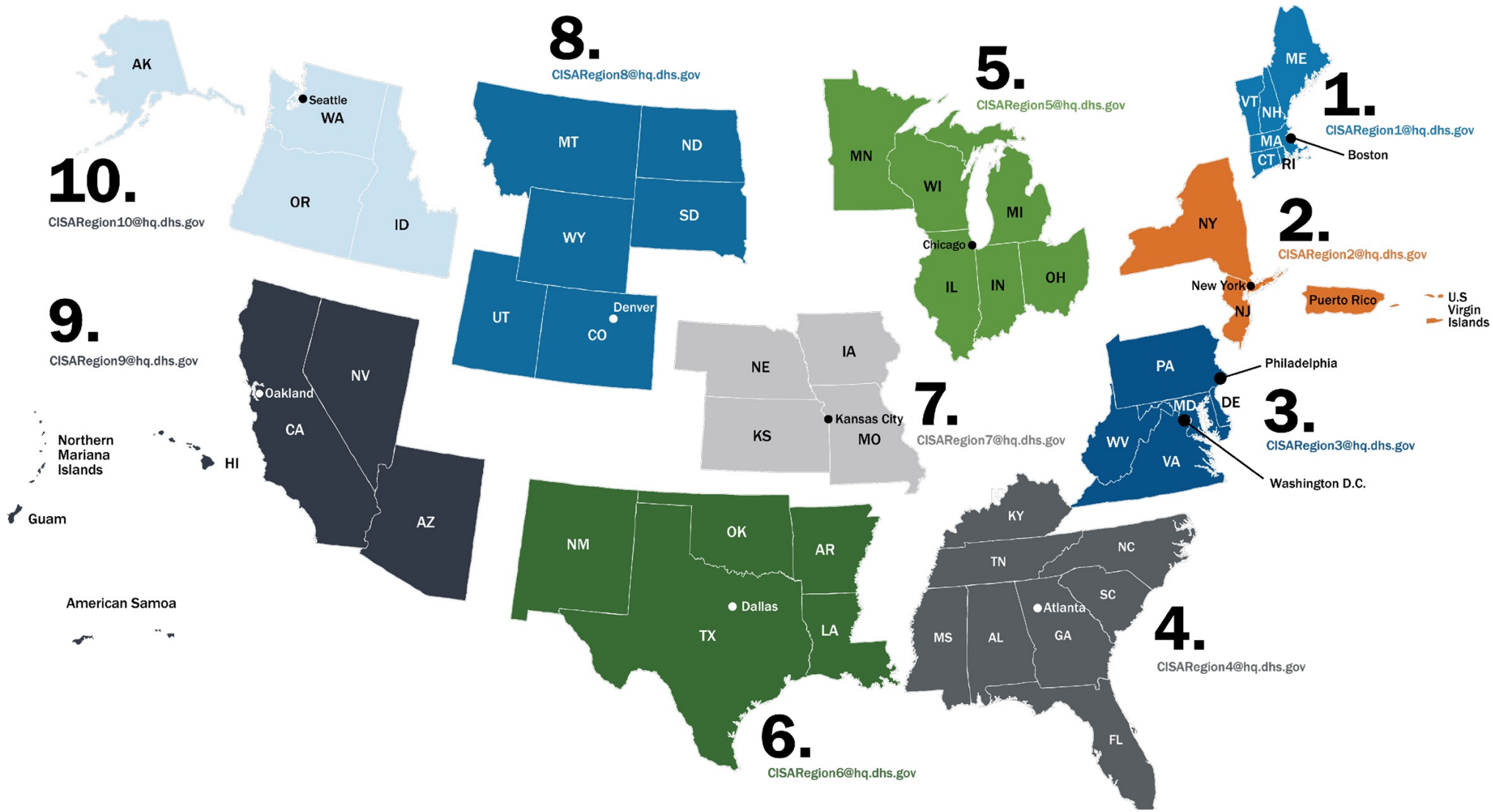
CISA mitigates the risk and enhances the resilience of our nation's critical infrastructure by preparing, planning, and managing operations and delivery of capabilities and services to support the defense and security of the nation's infrastructure.

HOW CISA IS CARRYING OUT ITS INTEGRATED OPERATIONS MISSION:

- Operational Visibility
- Integration of People, Disciplines, Organizations, Information
- Unified Regional Service Delivery

CISA Regions

- 1 Boston, MA
- 2 New York, NY
- 3 Philadelphia, PA
- 4 Atlanta, GA
- 5 Chicago, IL
- 6 Dallas, TX
- 7 Kansas City, MO
- 8 Denver, CO
- 9 Oakland, CA
- 10 Seattle, WA



Categorizing Threats

- Threat Sources
  - Nation-State Threats
  - Terrorism and Targeted Attacks
  - Climate Change and Extreme Weather
- Types of Threats
  - Physical
  - Cyber
- System Components
  - Offshore Turbines and Substations
  - Undersea Cables
  - Onshore Landing Sites and Substations

Potential Threats to Offshore Wind Farms

- Vehicle-borne Improvised Explosive Device – land and water
- Extreme Weather – high winds, hurricanes, floods, earthquakes
- Cyber Attacks – malware, ransomware
- Physical Attacks – arson, sabotage, espionage
- Supply Chain – disruptions, vulnerabilities
- Insider Threat – malicious insiders
- Electromagnetic Pulses

Why Build Security and Resilience

- The nation's security and economic prosperity relies on having consistently working critical infrastructure to support our lives, our communities and our nation.
- We need to be certain that our critical infrastructure is secure and have confidence in our incident response and recovery no matter the threats or hazards we face. This is national resilience.
- Building national resilience requires a collaborative partnership between business and government, between individuals and the broader community. It is a civic duty where everyone, the private sector, government, and academia plays a role to make the nation stronger.

Key Steps to Building Resilience

- Identify Critical Assets and Map Dependencies - Determine the systems that are critical for ongoing business operations, and map out their key dependencies on technology, vendors, and supply chains.
- Assess Risks - Consider the full range of threats that could disrupt these critical systems and the specific impacts that such threats could pose to continuity of operations.
- Plan and Exercise - Develop incident response and recovery plans to reduce the impact of these threats to critical systems and conduct regular exercises under realistic conditions to ensure the ability to rapidly restore operations with minimal downtime.
- Adapt and Improve - Periodically evaluate and update response and recovery plans based on the results of exercises, real-world incidents, and an ongoing assessment of the threat environment.

CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE MONTH

For more information:

www.cisa.gov

central@cisa.dhs.gov

www.CISA.gov/ShieldsReady

Questions?

Craig Conklin

Associate Director

Infrastructure Assessment and Analysis

Email: Craig.Conklin@cisa.dhs.gov

Phone: (202) 657-2297